Keidanren
Policy & Action

サイバーセキュリティ対策の強化に向けた第二次提言

2016 年 1 月 19 日

一般社団法人 日本経済団体連合会

1. はじめに

世界中でサイバー攻撃による被害が深刻化している。国民の安全・安心を守るためには、サイバーセキュリティの確保が重要な鍵である。わが国においては、昨年1月にサイバーセキュリティ基本法が施行され、サイバーセキュリティ戦略本部が発足し、国家安全保障会議やIT総合戦略本部と緊密な連携を図るとともに、各省庁に対する権限が強化された。加えて、事務局である内閣官房の内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）の人員や予算の増加などにより、政府の推進体制が強化されている。新たな推進体制に対して、経団連は、重要インフラ等をサイバー攻撃から守るため、「サイバーセキュリティ対策の強化に向けた提言」を昨年2月に公表した。

一方、わが国では、政府機関や企業などに対するサイバー攻撃がますます増加している[1]。昨年5月に、サイバー攻撃により特殊法人日本年金機構から約125万件の個人情報が流出し、国民が安心した生活を送るため、対策の一層の強化が必要という認識が高まった。海外では、多くの国で通信、放送、金融等において、重大な障害が生じている。

また、サイバー空間はイノベーション創出により成長戦略を実現する重要な場となる。様々なモノがインターネットにつながるIoT（Internet of Things）による経済・社会の発展が期待される中で、ICTの利活用を進めるための対策が一層重要となっている。加えて、本年5月の主要国首脳会議（伊勢志摩サミット）や2020年の東京オリンピック・パラリンピックの安全な運営に向け、重大な局面に差し掛かっている。こうした課題について、昨年9月4日に、政府は新たなサイバーセキュリティ戦略を閣議決定した。

そこで、東京オリンピック・パラリンピックも踏まえた産学官の連携強化と経済界の具体的な取組みについて、経団連として第二次提言を取りまとめた。

2. サイバーセキュリティの意義

国民が安心して暮らせる安全な社会を実現するため、公的機関におけるサイバーセキュリティを確保しなければいけない。中央省庁に加えて、独立行政法人や、日本年金機構をはじめとする特殊法人などの活動は国民生活に密接に関わる。こうした公的業務を行う機関における総合的な対策の強化が重要である。また、今後、マイナンバー制度の導入など、国民の利便性を向上させる施策の展開にあたり、地方公共団体を含めた対策の充実も求められる。

産業界は、ICTの利活用を通じて経済・社会の持続的発展を目指している。IoT

[1] 政府機関への標的型攻撃の脅威件数は2014年度に前年度比で倍増した。（センサー監視等による通報件数は2013年度139件、2014年度264件。不審メール等の注意喚起件数は2013年度381件、2014年度789件。／出所：NISC資料）

により新たな産業やビジネスを創出するためには、インターネットに接続するシステムや製品の利用におけるサイバーセキュリティを確保すべきである。

サイバー攻撃により、企業の事業活動に支障が生じることや、情報漏洩により信用の毀損や競争力の低下を招くことなどのリスク[2]も高まっている。そこで、企業としてもサイバーセキュリティ対策を重視している。

世界経済の発展のために、サイバー空間において、国際的に自由な情報の流通が必須である。このため、インターネット上に展開されるデータが国境を越えて安全で円滑に移転できるよう、サイバーセキュリティを確保する必要がある。また、セキュリティ対策を理由に国際的な貿易のルールを侵害する措置を是正すべきである。

3. サイバーセキュリティ対策

(1)情報共有

社会全体としてサイバー攻撃に対する強靭性を高めていくには、政府機関や企業が連携して、攻撃の脅威および適切に対処したベストプラクティスなどの情報共有を進めることが第一歩となる。官民連携においては、企業からの攻撃情報などの提供に対して、政府からも独自に入手した脅威情報や分析結果などを提供する双方向の情報共有が求められる。

民間企業間の連携においては、業界ごとの既存の情報共有の仕組みを他の業界に拡大することや、業界横断的な連携が必要である。業界ごとの情報共有については、通信や金融において、ISAC[3]が既に設立されている。このような取組みを他の業界でも進めるための支援を官民挙げて行うべきである。特に、重要インフラである 13 分野（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油）において、こうした仕組みを用いた情報共有を推進する必要がある。また、重要インフラに関連する企業における CSIRT[4]間の連携を進め、情報共有、事案対処、訓練を行う必要がある。そのため、セプターカウンシル[5]の運営および活動には引き続き NISC の支援が求められる。

重要インフラ以外の企業においても、ISAC や CSIRT のように情報共有･分析や事案に対処することで、社会全体のサイバーセキュリティを高めることになる。

---

[2] サイバー攻撃の被害者が、第三者に攻撃する加害者となるリスクも含む。

[3] ISAC（Information Sharing and Analysis Center）：セキュリティに関する情報を共有・分析する機関。

[4] CSIRT（Computer Security Incident Response Team）：コンピューターのセキュリティに関する事案に対処するチーム。

[5] セプターカウンシル（CEPTOAR（Capability for Engineering of Protection, Technical Operation, Analysis and Response）- Council）：重要インフラの各分野の代表で構成される情報共有・分析のための協議会。

政府や関連組織に対して企業が適切な情報を提供するためには、機密情報を保全する仕組みが求められる。例えば、情報の匿名化などによる情報提供のあり方について、官民および民間企業間[6]において合意することが必要である。

(2)人材育成

サイバーセキュリティを支える根幹は人材であり、重要インフラ分野を中心とした各業界において人材の採用と育成が求められる。まず、産業界が果たす役割を踏まえた人材の要件を明確化することが重要である。情報システム運用の担当者のみならず関係部門において事案に対処できる人材を育成することも必要となる。加えて、技術的な知見を有する人材だけでなく、法律、経済、国際政治などの知見を有する人材も必要となる。こうした課題を踏まえ、重要インフラ分野を中心とした主要企業 40 数社による「産業横断サイバーセキュリティ人材育成検討会」[7]において、日本の業界・企業の特質や実情に即した人材要件の検討が行われている。

大学や高等専門学校等の教育機関においては、求められる人材のレベルに応じた教育が求められる。また、各地方の大学がそれぞれの強みを活かして地方公共団体や地元の企業などと連携して人材を輩出することは、サイバーセキュリティの意識の向上や地方創生にもつながる。さらに、初等中等教育においては、リテラシーの向上や技術を正しく活用するための倫理観の醸成が必要となる。

教育機関が輩出した人材を評価する仕組みや基準を策定することで、企業は求めるレベルに応じた専門職を採用しやすくなるとともに、キャリアパスを明確化できる。また、情報セキュリティスペシャリスト試験をベースとした登録制度の創設、情報セキュリティマネジメント試験の導入をはじめ、国内外の資格制度の活用も有効である。

企業における人材の活躍を推進するためには、評価や処遇を見直す必要がある。トップ人材やホワイトハッカーに加えて、セキュリティに関わる実務レベルの運用・マネジメントの従事者からシステムの開発者に至るまで、広範囲な人材に対する評価の明確化およびキャリアパス形成が必要となる。一方、政府においても、専門性に応じた適切な処遇等により優れた人材を登用すべきである。

また、企業における既存の人材の能力向上と活躍や、組織の見直しなども重要となる。能力、専門領域、業務内容に応じて多様な人材が必要なことから、育成

---

[6] 金融 ISAC では、情報の提供元が、当該情報の共有範囲を指定できるルールを制定している。

[7] 「産業横断サイバーセキュリティ人材育成検討会」中間報告書（http://cyber-risk.or.jp/sansanren/）。

と維持ができるエコ・システム [8]の構築に産学官が一体となって取組む必要がある。

(3)セキュリティレベルの高いシステムの構築

①社会システム

情報通信、電力、金融などの重要インフラは国民生活や経済活動に大きな影響を及ぼすサービスを提供する社会システムであり、その機能が停止または低下することがないよう、官民が緊密に連携して重点的に防護していく必要がある。

重要インフラに対しては、サイバーセキュリティ対策の強化や範囲の見直しなどが必要となる。例えば、ITS[9]やスマートシティーを重要な社会インフラとして追加することや、実効性の確保の観点から重要インフラの周辺施設も含めることなどが考えられる。

また、効果的なセキュリティシステムの構築や演習・訓練のため、重要インフラに関するリスク分析が必須である。

政府や重要インフラへの大規模なサイバー攻撃により、国民の生活が大混乱に陥るといった有事の際には、適材適所で必要となる高度人材が産学官の間で柔軟に動ける仕組みが重要となる。

②技術開発とシステム運用

脅威の進化や IoT などの進展による多様なシステム連携に対応し、発生した攻撃に迅速に対処できる技術開発とシステム運用が必要である。情報システムだけでなく、インターネットと接続していない制御系システムについても対策の強化が必要となる。

技術開発課題については、悪意のある通信の検知や挙動分析、攻撃予兆解析、情報共有技術、システム機能維持、情報保護、情報匿名化、早期復旧などが挙げられる。政府の第 5 期科学技術基本計画においても、これらが重要な技術開発課題として明記されることを期待する。

運用については、システムを安定的に稼働させるため、サイバー攻撃を想定した日常の運用が重要になる。例えば、システム稼働や各種ログなどの情報の保全や活用等がある。

また、攻撃に対する完全な防御が困難であることを踏まえ、迅速な対応などにより被害を極小化することも重要である。

---

[8] 人材育成・維持のためのエコ・システム：産業界において、ICT 企業やセキュリティ関連事業者だけでなくユーザー企業においても、それぞれに必要なセキュリティ人材が雇用・維持されるような、産学官の連携による育成と雇用の仕組み。（「産業横断サイバーセキュリティ人材育成検討会」中間報告書）参照。

[9] ITS（Intelligent Transportation Systems）：高度道路交通システム。

こうした技術開発やシステム運用に対する民間企業の取組みに対するインセンティブを検討する必要がある。

上記の課題について、内閣府を中心として関係省庁が連携して進めている戦略的イノベーション創造プログラム（SIP：Cross-ministerial Strategic Innovation Promotion Program）の「重要インフラ等におけるサイバーセキュリティの確保に向けた研究開発計画」の社会実装に向けた取組みに期待する。また、官民が連携して進めている IoT 推進コンソーシアムにおいて、セキュリティの高いシステムの検討が求められる。

(4)国際連携の推進

サイバー攻撃の主体はグローバルに活動しており、国際テロ組織による攻撃も増加する中、国際的な連携の推進がまず必要である。他国で生じた攻撃への対処に関して、政府が入手した情報をそのまま企業に提供することは難しいが、可能な範囲で政府から最新の情報が提供されることが、高度な攻撃への対応を事前に準備するために必要となる。

国際連携の推進に向けて、わが国として、サイバー空間における国際的に自由な情報の流通を確保するため、サイバーセキュリティに係る国際的な議論への官民を挙げた積極的な参画が求められる。

また、政府は安全保障分野における他国との連携の強化に努めるべきである。米国とは、昨年 4 月に日米両国政府が改定した「日米防衛協力のための指針」に、サイバー防衛協力の推進が初めて盛り込まれた。これに加えて、インターネットエコノミー政策協力対話やサイバー対話を充実させ、官民における人材交流や、情報共有、共同訓練、技術開発などに取組む[10]べきである。

欧州とは、情報共有に関する制度[11]の整備を踏まえた官民の意見交換などに取組むべきである。ASEAN やアジア大洋州地域の諸国とは、サイバー分野における人材育成を含めた能力構築（キャパシティビルディング）のための国際協力が必要である。今後は、中南米や中東アフリカとの情報共有も可能な限り進めるべきである。

---

[10] 2015 年 12 月にワシントン D.C. で開催された「第 52 回日米財界人会議」の共同声明では、日米の政府と産業界がサイバー分野において官民連携などの協議を行うべきとされた。

[11] ネットワーク・情報セキュリティ指令（Network and Information Security Directive)に基づき重要インフラ業者やサービス提供者に対して事業報告の義務付けの方向性が示された。

(5)東京オリンピック・パラリンピックへの対応

2020 年には、東京オリンピック・パラリンピックが開催される。これを成功させることが、わが国が国際ビッグイベントを開催するうえでの試金石となる。今後、サイバー攻撃の増加が懸念される中、大会会場やそれに直接関わるシステムに加えて、周辺施設や間接的に関わるシステム等を含めた総合的な対策が求められる。

まず、関係企業が CSIRT を設置してサイバー攻撃に備えた情報共有ネットワークを強化するとともに、中核となる CSIRT を政府または組織委員会の下に直ちに設置すべきである。次に、様々な攻撃を想定し、攻撃検知や防御を連携して行うため、政府機関、中核となる CSIRT をはじめ関連組織が参加して、演習・訓練を着実に実施することが求められる。こうした実践により、組織への攻撃に関する情報や対処が速やかに共有され、新たな攻撃の阻止や被害の軽減が実現される。

2020 年の東京オリンピック・パラリンピックを取り巻くサイバー攻撃の脅威に対処できる人材は、学生の育成だけでは間に合わず、産業界の既存の人材の能力を向上させるのが効果的な方策である。産業界において潜在能力が高い人材を見つけ出し、基礎知識を深め、実地研修などの充実を図ることにより、人材を強化できる。政府や教育機関には、企業が人材を養成するにあたってのインセンティブや教育・訓練の提供などが求められる。

NISC を中心として、政府や関係機関は、こうした体制整備や必要な対策に関する詳細なロードマップを早急に策定し、全力を挙げて実行すべきである。

東京オリンピック・パラリンピックのために整備した基盤は、2020 年以降もわが国をサイバー攻撃から守るために活用できる。

4. 産業界の取組み

産業界としては、サイバーセキュリティの確保を経営上のリスク管理の重要項目として位置付け、これを周知し、経営層の意識を改革する。

具体的には、CISO[12]などとそれを支える組織・体制の整備、情報共有、人材育成、システム強化などへの取組みを自主的かつ迅速に推進する。セキュリティ人材の採用と育成に関しては、キャリアパスや処遇も考慮し、人材育成エコ・システムの構築に取組む。昨年 12 月に政府が策定した「サイバーセキュリティ経営ガイドライン」を参照し、企業の管理体制を整備してルールの遵守や社員のリテラシー向上を図る。セキュリティ関係の部門と他の関連部門が緊密に連携できるよう、組織の見直しなどを行う。あわせて、自社にとどまらず、サプライチェーンを含めた対策にも取組む。

ステークホルダーへの説明責任の観点から、情報開示が企業価値を高める側面もあることも踏まえ、サイバーセキュリティの取組みに関する情報開示を自主的

[12] CISO（Chief Information Security Officer）：最高情報セキュリティ責任者。

に進める。

ビジネスの面では、セキュリティ・バイ・デザインの考え方に基づくシステムの開発および運用、製品やサービスの提供を行う。また、リスク評価や補償範囲等の制度設計を引続き行い、サイバーセキュリティ保険を提供する。

こうした活動を通じて、産業界は、サイバー攻撃に強い社会システムを実現し、わが国のサイバーセキュリティの強化に貢献する。

以　上